DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") is entered into on _____ ("**Commencement Date**"),

BY AND BETWEEN: **SapiensIT Consulting GmbH**, a company incorporated under the laws of Austria, having its registered office at 1110 Wien, Sdlg. Neugebäude 5/116, with registration number 241892z

hereinafter called **"Sapiens"** or the "**Supplier**",

BY AND BETWEEN: _____

_____

_____

hereinafter called the "**Company**" or the **"Customer"**,

The Company and the Supplier are hereinafter referred to jointly as the "**Parties**" and individually as a "**Party**".

(1)
WHEREAS:

I. The Supplier provides the services hosted on addins.sharepointsapiens.com for Event Management for Office 365, Employee Training Management for Office 365, and Calendar E-mail Extension for Office 365 (hereinafter referred to as "Services"). In providing these Services, the Supplier may process personal data (as defined below) on behalf of the Company.

II. The Parties have concluded a main agreement regarding these Services (hereinafter referred to as "Master Services Agreement").

III. The Parties have hereunder agreed the terms upon which the Supplier will process such personal data.

THEREFORE, the Parties agree as follows:

Article 1. Data Protection

1.1. *Definitions:* In this Addendum, the following terms shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Law; and

(b) "**Applicable Data Protection Law**" shall mean: Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as well as, where applicable, any replacement or equivalent legislation of any other applicable jurisdiction, provided that the processing of personal data is actually governed by the national laws of such jurisdiction.

1.2. *Relationship of the Parties:* The Company (the controller) appoints the Supplier as a processor to process the personal data required for the performance of the Services as described in the Master Services Agreement (the "**Data**"). Each Party shall comply with the obligations that apply to it under Applicable Data Protection Law.

1.3. *Purpose limitation:* The Supplier shall process the Data as a processor for the purposes described in the Master Services Agreement and strictly in accordance with the documented instructions of the Company (the "**Permitted Purpose**"), except where otherwise required by any applicable law. In no event shall the Supplier process the Data for its own purposes or those of any third party.

1.4. International transfers: The Supplier shall not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("**EEA**") unless (i) it has first obtained the Company's prior written consent; and (ii) it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law (the "**Measures**"). Such Measures may include (without limitation) transferring the Data to a recipient in a country that the European Commission has decided provides adequate protection for personal data or to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law. In any case, the Supplier will only transfer the personal data outside the EEA according to the instructions of the Company. If the Supplier would process the Data outside the EEA and did not implement any Measure at

the time of execution of this Addendum, the Parties hereby agree that they will execute the Standard Model Clauses.

1.5. *Confidentiality of processing:* The Supplier shall ensure that any person that it authorises to process the Data (including the Supplier's staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process the Data who is not under such a duty of confidentiality. The Supplier shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

1.6. *Security:* The Supplier shall implement, at its own cost, appropriate technical and organisational measures to protect the Data against (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**"). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

1.7. Such measures shall include, as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1.8. *Subprocessing:* The Supplier shall not subcontract any processing of the Data to a third party subprocessor without the prior written authorisation of the Company. Notwithstanding this, the Company consents to the Supplier engaging (i) the subprocessors listed in Appendix 1 to this Addendum (ii) third party subprocessors to process the Data provided that: (i) the Supplier provides at least thirty (30) calendar days' prior notice of the addition or removal of any subprocessor (including details of the processing it performs or will perform); (ii) the Supplier imposes data protection terms on any subprocessor it appoints that protect the Data to the same standard provided for by this Addendum; and (iii) the Supplier remains fully liable for any breach of this Addendum that is caused by an act, error or omission of its subprocessor. Upon the Company's request, the Supplier shall

provide a copy of any agreement entered into with a subprocessor in accordance with this Addendum.

1.9. If the Company refuses to consent to the Supplier's appointment of a third party subprocessor on reasonable grounds relating to the protection of the Data, then either the Supplier will not appoint the subprocessor or the Company may elect to suspend or terminate the Master Services Agreement.

1.10. *Cooperation and data subjects' rights:* The Supplier shall provide timely assistance (including by appropriate technical and organisational measures) to the Company, at its own expense, to enable the Company to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. If any such request, correspondence, enquiry or complaint is made directly to the Supplier, the Supplier shall promptly inform the Company providing full details of the same.

1.11. *Data Protection Impact Assessment:* If the Supplier believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform the Company and provide the Company with all such reasonable and timely assistance as the Company may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

1.12. *Security incidents:* Upon becoming aware of a Security Incident, the Supplier shall inform the Company without undue delay and, in any case, within twenty-four (24) hours. In such case, the Supplier shall provide all such timely information and cooperation as the Company may require in order for the Company to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. The Supplier shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep the Company informed of all developments in connection with the Security Incident.

1.13. *Deletion or return of Data:* Upon the Company's request and the latest upon termination or expiry of the Master Services Agreement, the Supplier shall (at the Company's election) destroy or return to the Company all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing). This

requirement shall not apply to the extent that the Supplier is required by any applicable law to retain some or all of the Data, in which event the Supplier shall isolate and protect the Data from any further processing except to the extent required by such law. The Supplier shall provide the Company written confirmation of its compliance with the foregoing.

1.14. *Audit:* The Supplier shall permit the Company (or its appointed third party auditors) to audit the Supplier's compliance with this Addendum, and shall make available to the Company all information, systems and staff necessary for the Company's (or its third party auditors) to conduct such audit. The Supplier acknowledges that the Company (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that the Company gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to the Supplier's operations. The Company will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) if the Company believes a further audit is necessary due to a Security Incident suffered by the Supplier.

1.15. *Indemnity:* Each Party (the "**Indemnifying Party**") shall indemnify the other (the "**Indemnified Party**") from and against all loss, cost, harm, expense (including reasonable legal fees), liabilities or damage ("**Damage**") suffered or incurred by the Indemnified Party as a result of the Indemnifying Party's breach of the data protection provisions set out in this Addendum, and provided that: (i) the Indemnified Party gives the Indemnifying Party prompt notice of any circumstances of which it is aware that give rise to an indemnity claim under this Addendum; and (ii) the Indemnified Party takes reasonable steps and actions to mitigate any ongoing Damage it may suffer as a consequence of the Indemnifying Party's breach.

Article 2. Duration

2.1. This Addendum shall enter into force upon the Commencement Date and is concluded for the duration of the Master Services Agreement. Upon the termination or expiration of the Master Services Agreement, for any reason whatsoever, this Addendum shall automatically be terminated.

Article 3. Miscellaneous

3.1. Except as specifically set forth in this Addendum, all terms of the Master Services Agreement shall remain in full force and effect. In the event of any conflict or inconsistency

between the provisions of the Master Services Agreement and this Addendum, the provisions of the latter shall prevail.

3.2. This Addendum constitutes the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, representations or understandings between the Parties relating to the subject matter hereof. For the avoidance of doubt, it is specified that this clause will not affect any Standard Model Clauses entered into between the Parties, unless otherwise agreed between the Parties.

IN WITNESS THEREOF, the Parties have executed this Addendum in two original copies, each Party acknowledging receipt of one.

For the Company	For the Supplier
_____	_____
Name:	Name: Michael Aigner
Function:	Function: Managing Director
_____	
Name:	
Function:	

Appendix 1 – Sub-Processors

The following table lists the sub-processors the Supplier currently uses.

Sub-Processor	Description
Microsoft	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland For customers in Europe, data will be processed in the Netherlands, West Europe. For customers in Australia / Pacific, data will be processed in New South Wales, Australia East For customers in the rest of the world, data will be processed in the USA, Virginia, East US Microsoft's Product and Services Data Protection Addendum http://aka.ms/dpa
Stripe.com	If the Company chooses to use credit card to pay the subscription fees, the collected data will be controlled and processed by stripe.com. Their Privacy Policy can be viewed at https://stripe.com/us/privacy
Mailgun.com	If the Company chooses to use the Supplier's mail service instead of the Company's Exchange online e-mail service, the Services send and receive e-mail through mailgun's API and infrastructure. Their Privacy Policy can be viewed at https://www.mailgun.com/privacy-policy/

Appendix 2 - Scope of Processing

This appendix describes the scope of Processing

Subject-Matter and Duration of Processing

The Supplier process personal data for the subject matter specified under the Master Services Agreement and until the Master Services Agreement terminates or expires, unless otherwise agreed upon by the parties in writing. The subject matter is determined by the Services to which the Company subscribes and the data which the Company provides to the Services.

Nature and Purpose of Processing

The Supplier will process Personal Data only to provide the Services, to fix and improve them and the Supplier will not collect, retain, use, or disclose the Personal Data for any other commercial purpose other than providing the Services.

The nature and purpose of Processing is determined by the Services to which the Company subscribes and the data which the Company provides to the Services. For instance:

1. Services process data provided by users to the Services (by adding or modifying an item in SharePoint), including Personal Data if provided, for example to enroll users into events or courses and to send calendar email invitations or other notification emails.

2. Services process email replies to calendar email invitations to update the enrollment and display the information to other users.

Types of Personal Data

The following personal data will be processed:

Email address and common name to send email notification:

The Services use the email address combined with the common name from
(a) the user account when enrolling internal users to an event or course or when adding internal users to an event (organizers, instructor, etc.) or
(b) the email address and full name entered when enrolling external users to an event or course or when adding external guest or instructors to an event. The email address is used to send email invitations and notifications to enrolled users or users added to the event (organizers, instructors, etc.). The e-mail address and common name is stored in lists in the Company’s SharePoint site and is under the Company’s control.

Email address and common name to handle incoming emails:

If an incoming email is a reply to a calendar invitation, the Services use the email address combined with the common name from the email sender to update the reply status and to add an entry to the communication protocol in a list in SharePoint.

Email address for license validation

Applies to the Event Management and Calendar Email Extension add-in.

The Services use the hashed email address of the user that creates or modifies events and topics to uniquely identify the user and to verify if the user has a valid license assigned. Sapiens stores this information as part of the Customer's license data.

Other Personal Data

The Company controls the types of Personal Data provided via the Services for Processing. The Company has the option to collect other Personal Data from end users when using the add-in, for example in the enrollment form. This data is stored in lists in the Company's SharePoint site and is under the Company's control.

Special Categories of Personal Data

None anticipated, but the Company controls the types of Personal Data processed via the Services.

Categories of Data Subjects

The Company controls the categories of Data Subjects to which the Personal Data relates. For instance, the Company may Process via the Services Personal Data that relates to the Company's current or prospective customers, employees or business partners.

External enrollments: This section applies to data external participants enter in the external enrollment form. The Services are intended for use by the Company. As a result, for much of the Personal Information the Supplier collects and processes in the external enrollment form, the Supplier act as a processor on behalf the Company. The Supplier is not responsible for the privacy or security practices of the Company, which may differ from those set forth in this agreement.

Appendix 3 - Technical and Organizational Measures

Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Sapiens implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1 Confidentiality

Physical Access to Facilities

- Personal Data is exclusively transmitted and processed in Microsoft Datacenters.
- Microsoft controls physical access to Datacenters.
- Access to Sapiens premises is limited to Sapiens personnel.

Access Policy

- Sapiens maintains a record of security privileges of individuals having access to systems that process Personal Data.
- Least Privilege Policy, Sapiens restricts access to systems that process Personal Data to only those individuals who require such access to perform their job function.

Access Authorization

- Sapiens maintains and updates a record of personnel authorized to access systems that process Personal Data.
- Sapiens deactivates authentication credentials that have not been used for a period not to exceed six months.
- Sapiens identifies those personnel who may grant, alter or cancel authorized access to systems that process Personal Data.
- Sapiens ensures that where more than one individual has access to systems processing Personal Data, the individuals have separate identifiers and logins.

Authentication

- Sapiens uses industry standard practices to identify and authenticate users who attempt to access information systems.
- Where authentication mechanisms are based on passwords, Sapiens requires the password to be at least eight characters long.
- Sapiens ensures that deactivated or expired identifiers are not granted to other individuals.
- Sapiens monitors repeated attempts to gain access to the information system using an invalid password.
- Sapiens maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.
- Sapiens uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.
- Whenever possible Sapiens forces Multifactor Authentication.

Confidentiality

- Sapiens instructs personnel to disable administrative sessions when leaving premises Sapiens controls or when computers are otherwise left unattended.
- Mobile Computers and Media must be encrypted.

2 Integrity

- Sapiens Software transmits Personal Data from the Customer's Data Storage encrypted and on customer's request and processes the data immediately. Personal Data is cleared from memory immediately after processing.
- Sapiens maintains separate environments for production, development, and testing.
- Sapiens uses self-generated sample data in testing and development environments.
- Software released and published for use by customers can only access production environments and is available in Microsoft stores. It has been verified by Microsoft's store submissions Team prior to release.
- Software under development and for testing can only access development and testing environments.

3 Availability and Continuity

Sapiens hosts services in Microsoft Data Centers only to assure high availability and continuity. Sapiens services are configured to scale-out to avoid overloading.